COMMUNITY IMMUNIZATION REGISTRIES MANUAL

CHAPTER II: CONFIDENTIALITY

Updated
February 2000

CONTENTS

The following CDC staff member prepared this report:

Gail A. Horlick, M.S.W., J.D.
Program Analyst
National Immunization Program

in collaboration with

Amy Fine, B.S.N., M.P.H.
Health Policy/Program Consultant, Washington, DC.
Member, National Vaccine Advisory Committee

and the Privacy and Confidentiality Implementation Team Members

All Kids Count Program
Ellen Wild, M.P.H.
Public Health Advisor

Centers for Disease Control and Prevention
National Immunization Program
Susan Abernathy
Program Analyst

Julie W. Gamez
Program Analyst

David B. Nelson, B.S.
Program Analyst

Glen J. Nowak, Ph.D.
Associate Director for Health Communications

Brian M. Willis, J.D., M.P.H.
Senior Public Health Advisor

State of California Department of Health Services
Immunization Branch
Ayesha E. Gill, Ph.D.
Statewide Immunization Information System Coordinator

Florida Department of Health
Division of Disease Control
Rae Hendlin
Medical Health Care Program Analyst

Henry T. Janowski, M.P.H.
Chief, Bureau of Immunization

Susan Lincicome
Senior Management Analyst II

Massachusetts Immunization Information System
Robert Rosofsky, M.A., Director
Bureau of Communicable Disease Control

National Vaccine Program Office
Daniel A. Salmon, M.P.H.

Rhode Island Department of Health
Kim Salisbury-Keith, M.B.A.
Deputy Chief Children's Preventive Services

Amy Zimmerman, M.P.H.
Chief, Office of Children's Preventive Services

ACKNOWLEDGEMENTS

The editor wishes to acknowledge the contributions of the following organizations: All Kids Count, The Task Force for Child Survival and Development; the Association of State and Territorial Health Officials and their affiliates; the Centers for Disease Control and Prevention; the National Association of County and City Health Officials; and the National Vaccine Program Office. In addition, personnel from various state, country, city, and local health departments, managed care organizations, health care organizations, and well as physicians in private practice contributed to this chapter. Among those individuals participating at different times were immunization program managers, attorneys, and privacy advocates.

The National Vaccine Advisory Committee of the Department of Health and Human Services approved this document on February 28, 2000.

INTRODUCTION TO CHAPTER II

One of the strategies to reach and sustain the goal of immunizing 90% of the nation's children who are under 2 years old by the year 2010 is to develop immunization information systems, referred to as "immunization registries."[1] Immunization registries are confidential, computerized information systems that contain information about immunizations and children. Registries permit health departments and providers to consolidate and maintain a computerized immunization record on children within a community. A proposed *Healthy People 2010* goal is to enroll 95% of children from birth through age five in a fully functional immunization registry.[2]

There are three primary purposes for the development of registries: (1) Registries may serve as a "reminder and recall" system for parents**.** Registries remind parents when their child is due for a vaccination, or contact the parents when the child has missed an appointment, or is overdue for an immunization. (2) Registries may serve as a clinical assessment and monitoring tool for providers. They can assist providers in identifying their patients who require an immunization in a timely manner, and forecasting which immunization(s) a child may require by incorporating the most current immunization schedule into the registry. In addition, immunization registries permit providers to exchange information on the immunization status of a child, benefitting children, parents, and providers. This may be necessary when the child receives medical services from several providers, is away from the medical home, or is seen in an emergency department. This will also ensure that immunization records are complete when a child receives immunizations from more than one provider. (3) Finally, from a public health perspective, registries may assist communities in the assessment of immunization coverage and the identification of pockets of need.

As of April 1999, 61 of 64 (95%) federal immunization grantees (50 states, D.C., 8 territories, and 5 cities) reported that they were developing or operating registries. Twenty-two of these grantees also reported an additional 103 independent registries.[3] The Robert Wood Johnson Foundation launched the All Kids Count project in 1991 to develop vaccine tracking and monitoring systems for preschool children. Other private foundations joined this effort, resulting in 24 funded projects, each of which worked to develop an automated immunization registry to monitor immunization status, identify service gaps and barriers, and establish follow-up and referral mechanisms. The Robert Wood Johnson Foundation is currently funding All Kids Count II, in which 16 of the most fully developed registries in the country are receiving additional support to become fully operational by January 1, 2000. All Kids Count defines a "fully operational" registry as a registry which contains 95% of 0-2 year old children in a given geographical area, with immunization events on 95% of those children, and has 90% of all providers in the area submitting immunization data to the registry. A fully operational registry also generates reminder or recall notices, produces population-based immunization coverage analysis, and has a written confidentiality policy.

Protecting the privacy of registry participants and the confidentiality of information contained in registries are major concerns for registry developers. The terms privacy, confidentiality, and security are often used interchangeably; the distinction between these terms and how they are applied must be clear. The following definitions for these terms are used in this document:

Privacy is the legal right of an individual to limit access by others to some aspect of the person.[4]

The Institute of Medicine report states, that the term “privacy” can include three privacy interests: first, autonomy, or decisional privacy, which protects fundamental constitutional liberties related to private behavior; second, protection against surveillance or intrusion where there is an expectation of privacy, e.g., protection against unlawful searches; and third, informational privacy, which concerns “the interest of the individual in controlling the dissemination and use of information” about oneself.[5]

Confidentiality is the treatment of information that an individual has disclosed in a relationship of trust with the expectation that it will not be divulged to others in ways that are inconsistent with the understanding of the original disclosure.[6]

Security encompasses a set of technical and administrative procedures designed to protect data systems against unwarranted disclosure, modification, or destruction.[7]

Individually identifiable information is information that identifies the individual, or can reasonably be used to identify the individual.[8]

Additional terms are defined in the **glossary.**

The individual’s right to privacy and the protection of confidential information contained in immunization registries are so critically important that the editor believes a separate chapter on the subject is demanded. These issues pose significant and urgent challenges to immunization registries as they are developed and operate on a daily basis. Media attention and recent legislation have further accentuated public sensitivity in this area. Officials in all fields are increasingly called upon to account for violations or perceived violations of individual privacy. In an increasingly litigious society, lack of adequate attention to this crucial area of concern could have severe consequences for the registry and its operators.

In response to these concerns, recommendations addressing confidentiality issues of immunization registries were developed by the Centers for Disease Control and Prevention (CDC), the All Kids Count Program, and the National Vaccine Advisory Committee (NVAC). The original Community Immunization Registries Manual chapter on Confidentiality was approved by NVAC in January 1997. This document revises and updates the 1997 chapter in light of the following significant events:

> The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191) was enacted. HIPAA requires Congress to enact federal privacy legislation by August 21, 1999 or the Secretary of the Department of Health and Human Services is to promulgate regulations to ensure the confidentiality of certain health care information by February 2000. Since Congress did not meet this deadline, the Department of Health and Human Services published draft privacy regulations in the Federal Register on November 3, 1999. The 60 day period for public comments was extended 45 days until February 17, 2000. The final rule will be published after an extensive review of the comments. Congress may still enact privacy legislation.
>
> In September 1997, Department of Health and Human Services Secretary Shalala (Secretary) issued recommendations to Congress for national privacy legislation. These recommendations reflect the concept that individuals should have certain basic rights in

regard to their medical records, including the right to find out what information about them is in a record and how the information will be used.[9]

In July 1997, President Clinton directed Secretary Shalala "to start working with the states on an integrated immunization registry system".[10] As a result, an Initiative on Immunization Registries was undertaken by the NVAC with support from the National Immunization Program of the CDC, and the National Vaccine Program Office.

A Workgroup including representatives from provider organizations, managed care plans, state and local health departments, parent and consumer groups, and the health information system community was formed to facilitate the development of a nationwide network of community- and state-based immunization registries. The Workgroup identified privacy and confidentiality as one of four key issues to be addressed by the Initiative.

The Workgroup convened four public meetings attended by more than 400 persons, with 104 persons providing expert testimony. To ensure input from a representative cross-section of parents, at the request of the Workgroup, the CDC National Immunization Program sponsored 21 parent focus groups.

On January 12, 1999, the NVAC approved the report entitled "Development of Community- and State-Based Immunization Registries". The report describes the vision, mission, goals, and objectives of immunization registries, and recommends specific action steps for the successful implementation of a network of community- and state based immunization registries. The vision guiding the NVAC recommendations is a nation with all children appropriately protected against vaccine-preventable diseases.

To implement the recommendations, the 1999 NVAC report recommended that a team develop minimum specifications for protecting the privacy of immunization registry participants and the confidentiality of the information contained in immunization registries. In February 1999, a CDC-led Privacy and Confidentiality Implementation Team with representatives from All Kids Count, the National Vaccine Program Office, and state registry projects was formed to achieve this goal; NVAC also provided extensive input.

This revised chapter includes minimum specifications for protecting the privacy of registry participants and the confidentiality of information contained in the registry, and guidelines for implementing the minimum specifications. It is intended to provide guidance to immunization registry developers and users. The principles in this document are consistent with HIPAA, Secretary Shalala's recommendations to Congress for privacy legislation, and the NVAC recommendations.

The privacy of immunization registry participants and the confidentiality of information contained in an immunization registry must be addressed within the context of the topics discussed in the other three chapters of the All Kids Count/CDC Community Immunization Registries Manual: **Planning** (Ch. I), **Technology** (Ch. 3), and **Operations** (Ch. 4). Confidentiality and the above three topics impact and influence each other. Appendix D contains updated security information.

One of the greatest challenges in developing an immunization registry is balancing the need to gather and share information to protect the health of the public and provide clinical benefit to individual children, with the necessity of protecting the privacy of patients, providers, and other system users. To provide individual clinical benefit, immunization registries must share information among providers and other authorized users in order to ensure that children are age-appropriately immunized. Implicit in the concept of a registry is the sharing of information between providers and other authorized users without the necessity for a traditional provider-to-provider request. To be an effective public health tool, registries must collect immunization information and share some basic demographic information to ensure that the population is adequately immunized, and to prevent the transmission of vaccine-preventable diseases. In addition, researchers, service organizations, policy makers, quality care organizations, managed care organizations, public health practitioners, and others, may have legitimate needs for access to information contained in the immunization registry.

An individual's medical, demographic, and financial information is both personal and confidential. An immunization history should include the date and type of vaccine administered, the dose, the vaccine lot number, and the vaccine manufacturer, although it is not required that all this information be contained in the registry. Potentially sensitive information such as the existence of contraindications, adverse reactions, or objections to immunization should also be part of the immunization history, though it is not required that all this information be contained in the registry. Demographic information includes name, address, telephone number, date of birth, and gender. To many people such as immigrants and those avoiding domestic violence, it may be more important to protect their demographic information than their immunization information from disclosure. An immunization record may also contain potentially sensitive financial information, including a person's insurance status and/or use of or enrollment in government assistance programs.

Public Hearings and Parent Focus Groups

Testimony at the public hearings from representatives of advocacy and parent groups included concerns about the privacy and confidentiality of immunization registries, and the potential for the improper use of information. While some parents expressed support for the benefits that immunization registries can provide, other people expressed concern about the potential use of demographic data to track families for purposes other than immunization, such as the tracking of undocumented immigrants by the Immigration and Naturalization Service (INS), or to locate a child or a parent in cases of domestic violence. Some leaders of the Hispanic health advocacy community (the National Coalition of Hispanic Health and Human Services Organizations (COSSMHO) expressed reservations about registry development because of the potential to further marginalize underserved populations including immigrants, migrants, and Hispanic families.

Others expressed concern about the potential use of information to deny government services, or to harass or punish parents who chose not to immunize. Concerns were also raised about linking immunization data to other health information that would lead to the denial of health insurance or services. In addition, some expressed concern about government intrusion into family decisions about health care. There was a strong, consistent message from those testifying that narrowing and focusing the scope and use of registry information would best protect patient privacy and confidentiality.

Findings from the focus groups across the nation also indicated that parents recognized the importance of protecting privacy and confidentiality. Most people expressed a positive reaction to the idea of an immunization registry, although some people questioned the need for some of the information or wondered if the information could be misused. However, participants most commonly named the possibility of a breach in confidentiality and privacy as the issue about which they were most concerned. In contrast to the testimony at the public hearings, the focus group research found that "Hispanic groups were more open (than other race/ethnic groups) to allowing a wider variety of individuals and organizations to have access to the information in the registry."[11] Some participants were in favor of linking the registry to other health care databases, such as those kept by Women, Infants and Children (WIC) Nutrition Supplement Programs and Medicaid, while others did not like the idea.[12]

Legal Protection of Confidential Health Care Information

The confidentiality of information in an immunization registry may be governed by Federal, State, or local laws or regulations. The Freedom of Information Act and the Privacy Act of 1974 protect name-identified information from disclosure by the Federal government without the consent of the individual named.

State laws provide varying protection for registry related information, and the interstate exchange of immunization records is a major challenge for registry developers. Disease specific state statutes such as AIDS/HIV laws protect certain types of information. Professional practice acts, hospital licensure laws, and civil and criminal statutes also protect confidential health care information. Most of the existing laws need review because they were developed before the rapid advances in technology, and they do not address an interstate health care delivery system or electronic information systems.

In many states, immunization-related information is considered part of the confidential patient medical record. Information that is considered public health data may be defined under existing state public health laws. Certain circumstances may require special provisions for the protection of immunization-related information. If the registry is operated in conjunction with a health department, but is actually administered by a non-profit organization, the immunization-related information in the registry may not be protected under the state public health laws. A number of public health departments have contracted with the private sector to assist in the development of the immunization registry. Public health laws often apply only to information maintained by the health department. If the information is not protected by the public health laws, it must be determined whether state laws on confidentiality of medical records apply, whether new legislative or administrative actions are required, or whether certain requests for access to, or use of the information must be denied under existing laws.

The Need for Confidentiality Policies

The public health community has a long history of protecting individual privacy and confidentiality when handling sensitive and personal information. The emergence of new technologies makes it easier to collect, transmit, and store personal information. Legislation and technical security measures are important means of protecting privacy and confidentiality, but they are not sufficient. Registry participants must feel confident that their health care information is protected from unauthorized access and disclosure, and that information will be

used for the purpose for which it was collected.

Policies and procedures also minimize potential liability. Most breaches in confidentiality are intentionally or inadvertently caused by someone with legitimate access to the system.[13] It is important to be proactive rather than reactive; in the event of a lawsuit, the court is likely to ask what steps have been taken to protect confidential information. Furthermore, most of the proposed bills for federal privacy legislation require that administrative safeguards be implemented; such safeguards include confidentiality policies.

Immunization registry developers and managers are in a position to provide leadership for the continued protection of an individual's personal information by establishing standards that maintain privacy and confidentiality while simultaneously using technology to improve the public's health and safety. Registry developers must implement policies and procedures to protect participants' privacy and to minimize liability. Clearly delineating how specific issues will be handled and educating registry users are important safeguards against breach of confidentiality through inadvertent or intentional abuse. Providers and their staffs must constantly be vigilant not to indiscriminately disclose information about their patients without the patient's authorization, or as required by law. Health officials can increase community confidence and participation in the system by ensuring the public of the following:

Information in the system will be used in ways consistent with the purpose of ensuring that children will be vaccinated on time.

Only authorized users will have access to information in the system.

Disclosure of information to authorized users will only be on a "need to know" basis.

Information will be released for the exclusive purpose for which it is requested.

Registry information must be complete and accurate; if it is not, parents and providers will lose confidence in it and cease to participate in registries. The more detailed personal information is, the greater the probability it will contain items that could be harmful to an individual if inappropriately disclosed. This chapter has been prepared specifically to aid the registry developer and manager in achieving that delicate balance between the individual's need for privacy and the clinical and public health need for information, and to ensure that the public health community's high standards for personal protection are continued in the new age of rapid information exchange.

1: GUIDING PRINCIPLES

The confidentiality policies in this chapter are designed to protect the privacy of registry participants and the confidentiality of individually identifiable information contained in the registry. Non identifiable, aggregate immunization registry information may be used to identify areas with low immunization coverage rates and to promote health and prevent disease. The confidentiality policies in this chapter are based on the following important principles:

1. The protection of privacy and the maintenance of confidentiality are essential to the successful development of immunization registries[14].

2. The confidentiality policies in this chapter are designed to balance the clinical and public health need for information and the privacy rights of the individual.

3. The confidentiality policies in this chapter are based on the principles of fair information practice, including the individual's right to know what information about him or her is in a record and how it is used, and to request amendments or corrections to the record.[15]

4. An immunization registry is a tool for monitoring and improving population-based health as well as the personal health of individuals. The information contained in the registry provides immunization decision support. Registries do not replace parental or provider responsibility.

5. The decision whether or not to participate in the registry and the decision whether or not to vaccinate are separate and distinct decisions.

6. All immunization registries, including registries that are part of integrated information systems, must ensure that privacy is protected.[16]

2: CONFIDENTIALITY SPECIFICATIONS AND GUIDELINES

The minimum specifications and implementation guidelines that follow are based on the NVAC recommendations, the experience of registry developers in the public and private sector, as well as that of representatives from CDC, the National Immunization Program, All Kids Count, state and local health departments, and others. The minimum specifications provide a standard of protection for the privacy of immunization registry participants and for the confidentiality of the information contained in the registry. Experience gained from immunization registry projects indicates that registries must be tailored to meet local needs. The implementation guidelines include different ways of implementing the minimum specifications in order to ensure that registry developers use approaches that are most consistent with the community values of the population being served by the registry. To be in compliance with national confidentiality policies for immunization registries, registries must comply with the minimum specifications that follow.

1. CONFIDENTIALITY POLICIES

A. Minimum Specifications for Confidentiality Policies:

1. Every immunization registry must have a written confidentiality policy that will be made available upon request.

2. The confidentiality policy must be reviewed to ensure that it is consistent with applicable Federal, State, and local laws and regulations.

3. Confidentiality policies must apply to everyone who has authorized access to the registry.

4. Confidentiality policies must apply to all individually identifiable information in all formats including paper-based and electronic records.

5. Confidentiality policies must prohibit the unauthorized redisclosure of personally identifiable information.

6. Confidentiality policies must:
   clearly define the user's responsibility to maintain confidentiality
   clearly define what constitutes a breach of confidentiality**,** and
   specifically delineate the penalties for the inappropriate use or disclosure of information.

7. Confidentiality policies must be actively enforced.

B. Implementation Guidelines for Confidentiality Policies:

1. Confidentiality policies are most successful when developed in collaboration with the communities they serve.

2. Policies should be clear and easy to understand, and materials designed for participants should be written with appropriate attention to language and cultural concerns.

3. Policies should be reviewed and updated on a regular basis to ensure that they are consistent with applicable legislation and regulations, and to ensure that they continue to reflect community standards and values.

4. Initial and periodic confidentiality training should be provided to all persons who have access to registry information to increase knowledge and awareness of appropriate behavior as well as any changes in the policy.

5. If a confidentiality policy does not address security, a separate policy should address technical security issues (see Appendix D).

2. AGREEMENTS TO PROTECT CONFIDENTIALITY

A user agreement defines the terms under which individuals and organizations become authorized immunization registry users. It includes the obligations and responsibilities of both parties (e.g., how the information is used, who provides user support).

A confidentiality statement is a written statement dated and signed by an individual which certifies that the individual has received a copy of the confidentiality policy, understands the terms, including the penalties for violation of the policy, and agrees to comply with the policy.

Some states use separate user agreements and confidentiality statements; other states incorporate a confidentiality statement in a user agreement. Individuals are also bound by any existing local, state or federal laws, regardless of whether they have signed a confidentiality statement or a user agreement.

A. Minimum Specifications for User Agreements and Confidentiality Statements:

1. All authorized immunization registry users must receive a copy of the confidentiality policy.

2. All individuals with access to the immunization registry must either:
   sign a confidentiality statement or a user agreement indicating that they understand the terms of the confidentiality policy, including the penalties for violation of the policy, and they agree to comply with the policy, or
   individuals must operate under an employer who has signed an agreement indicating that they are responsible for the actions of the staff (see implementation guidelines below).

3. Confidentiality statements and user agreements must specify the time period covered by the statement or agreement, and they must be renewed on a regular basis.

4. Confidentiality statements and user agreements must specify the user's level of access to information in the immunization registry.

B. Implementation Guidelines for User Agreements and Confidentiality Statements:

1. It is preferable for every authorized immunization registry user to sign a user agreement. However, it is sufficient for a provider to sign the user agreement for his or her staff, if the agreement addresses confidentiality obligations, and indicates that the provider agrees to be responsible for the actions of his or her staff regarding the confidentiality of information contained in the registry.

2. It is also sufficient for the staff in a provider's office to sign a general confidentiality agreement indicating that they will maintain the confidentiality of all patient information including the information in the immunization registry.

3. Non registry users with authorized access to the registry (e.g., technical support staff) should also sign a confidentiality statement.

3. NOTIFICATION

Notification informs patients and their parents or legal guardians of the purpose and potential uses of the immunization registry. Notice is an important aspect of the principles of fair information practices that were formulated by the U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems in 1973.[17] This principle continues to be relevant today. It is consistent with the principle of consumer control in the Secretary's recommendations, which states that Americans should have the right to find out what information about them is in a record, how the information will be used, and the right to inspect, copy, and if necessary, amend or correct their record.

A 1997-1998 CDC survey of state legislation related to registries which has been informally updated, indicates that most states provide some type of notice that immunization information is in an immunization registry and/or that it will be shared.[18] The testimony at the NVAC public hearings and findings from the parent focus groups indicate that the overwhelming majority of people want to be notified of the existence of an immunization registry. The concept of notice was frequently tied to a statement about choice regarding participation in the registry. While the concepts of notice and choice are closely related, this section addresses notice.

NVAC recommends that, "At a minimum, immunization registries should ensure that patients or parents are notified of the existence of the registry and of the information contained in the registry, and inform them of the purpose and potential uses of the registry."[19] The report also states that registries should permit patients and/or parents or legal guardians to review and amend information in the registry.[20]

A. Minimum Specifications for Notification:

1. Information about the existence of the immunization registry (notification/notice) must be provided directly to patients and/or their parents or legal guardians.

2. Notification must include the following:
   what information will be contained in the registry

what the information will be used for
with whom the information will be shared
the definition of participation in the registry and how to exercise choice about participation (see implementation guidelines for choice, page 13)
procedures for review and correction or amendment of information
contact information for further questions

3. Notification must be in language the parent or guardian can understand.

4. Information about the immunization registry must be given to the patient and/or parent or guardian before any immunization information is included in the registry.

5. In states where immunization registries are populated directly from vital records:
a) if only demographic information is transmitted, parents or guardians must be notified before any immunization information is included in the registry, and
b) if information on vaccines given at birth, such as HepB, is transmitted in addition to the demographic information, parents or guardians must be notified before this information is included in the registry.

6. If a parent or guardian signs a contract with a health care provider or health plan and that entity participates in the registry, the policy contract or health plan brochure does not provide sufficient notice. Providers must provide additional notice consistent with the minimum specifications.

B. Implementation Guidelines:

1. It is preferable to notify the parent or guardian before any information is included in the registry.

2. Explicit consent serves as notice if the consent form includes the minimum specifications for notice.

3. Methods of providing notice, include but are not limited to, notice on the vaccine administration form, vaccine information statement, or in a separate flyer, letter or brochure that is either mailed in advance or distributed during the clinical encounter (e.g., prenatal or pediatric visit).

4. Reasonable efforts to provide notice should be made. For example, if notice is mailed to the patient's last known address, and it is returned, reasonable additional attempts to provide notice should be made.

5. If verbal notice is given, it is helpful to have a written statement addressing the information to be disclosed, in order to ensure that consistent information is disclosed (see Appendix C for prototype language for disclosure used in California). It is good practice to accompany verbal notice with written documentation that notice has been provided.

6. Signs in waiting rooms, public service announcements and media campaigns about the

benefits of immunization registries are an important supplement to notice to an individual, but they are not a substitute for direct notice.

4. CHOICE

It is essential that once a parent or guardian has been notified of the existence of the registry, he or she has the ability to choose whether or not to participate in the registry. NVAC specifically recommends that "parents must be given the option to decide whether or not their children will participate in a registry".[21] NVAC also recommends that the option to "opt in" or to "opt out" of registries (see implementation guidelines below) should be consistent with community values.[22]

The findings from the parent focus groups indicate that most parents feel positively about registries when they understand the benefits. Many participants in the parent focus groups favored a law or policy that requires explicit consent of parents before information enters the registry. Many participants were least comfortable with a law or policy that requires automatic inclusion of children in a registry, but very few indicated they would actually opt out if given the choice. This is consistent with the findings from the updated 1997-1998 CDC survey of state legislation; when given the option, few parents choose not to participate in immunization registries.

The updated 1997-1998 CDC survey indicates that in 33 states, consent to be in the registry is implied; that is, a child's immunization information is included in the registry and/or shared without explicit authorization by a parent or guardian. In 24 of these 33 states, there are provisions that allow parents or guardians to either "opt out" of the registry or to limit access to the information contained in the registry. Nine of the 33 states do not provide an option to opt out or to limit access to the information contained in the registry. Fourteen state laws require explicit consent to participate in the registry. The remaining states had not yet addressed the issue of choice. A few states such as Michigan and Colorado, have laws that specifically require the registry to be populated directly from vital statistics.

A. Minimum Specifications for Choice:

1. Parents must be able to choose whether or not to participate in the registry, and they must be able to change this decision at any time (see notification page 11).

2. Parents and children must not be penalized for choosing not to participate in a registry for religious, philosophical, privacy or other reasons.

3. Personally identifiable information of those who have chosen not to participate must not be shared.

4. The options and benefits regarding participation (see implementation guidelines below) must be clearly explained to parents or guardians.

5. Verbal choice about participation in the registry must be documented.

6. The decision whether or not to vaccinate, and the decision whether or not to participate in registry are separate and distinct decisions. Therefore, separate signatures must be used to indicate consent or refusal to vaccinate, and for consent or opting out of participation in the registry.

B. Implementation Guidelines for Choice:

The following options for exercising choice are available to allow registry developers to implement approaches that are most consistent with the community values of the population being served by the registry:

1. Explicit consent or "opt in": Registries using this option will only include immunization information in the registry if the parent or guardian explicitly consents to participation in the registry. Consent may be written or verbal.

2. Implied consent or "opt out": Registries using this option automatically include all children in the registry unless a parent requests otherwise. A parent or guardian who does not wish to participate may choose to "opt out". Verbal or written methods of opting out are used.

3. "Locked or restricted access": Registries using this option keep the demographic and immunization information in the registry but upon the request of the parent or guardian, it is not shared. Some registries allow parents broad discretion in exercising this option (e.g., do not share with a particular provider or anyone); other registries narrowly limit the opportunity to restrict access.

4. Some registries give parents or guardians the option to opt out of certain aspects of the registry such as reminder or recall notices.

5. USE OF IMMUNIZATION REGISTRY INFORMATION

The Secretary's recommendations state that with very few exceptions, health information should only be used for purposes compatible with and directly related to the purposes for which the information was collected or received. Other uses can be made only with patient authorization, or as allowed by law. In addition, all uses and disclosures should be restricted, to the extent practicable, to the minimum amount of information necessary to accomplish the purpose for which the information is used or disclosed.

Testimony at the public hearings consistently indicated that narrowing the scope and use of registry data would best protect privacy and confidentiality. Immigrant advocacy and consumer groups expressed concern about the potential for the improper use of immunization registry data that could result in the denial of benefits or services, or jeopardize the safety of the child or the family in a situation involving domestic violence. Concern was expressed about potential INS use of Social Security numbers and other demographic data (including a parent's place of birth or address) to track undocumented immigrants, or the use of data by estranged parents to locate family members in abusive situations. Thus, the NVAC recommendation states, "use of registry data in a manner that is punitive to parents/patients (e.g., denial of health

insurance/coverage, INS tracking of immigrants, other law enforcement purposes) must be prohibited."[23]

Non identifiable, aggregate immunization registry information is used for: 1) the identification of geographic regions with low immunization coverage rates (i.e., "pockets of immunization need"), and 2) the development and implementation of other infant and child health promotion or disease prevention interventions (e.g., outreach for lead screening).

A. Minimum Specifications for Use of Immunization Registry Information:

1. Each registry must identify the purposes for which it is collecting immunization information, and inform all authorized users and parents or guardians.

2. Information in the immunization registry must only be used for the purposes for which it was collected.

3. Immunization registry developers and managers must make every reasonable effort to ensure that immunization information is not used in a punitive manner (e.g., to deny services or to track immigration status). (See minimum specifications for disclosure).

4. Providers must be notified and given the opportunity to consent if immunization registry information that identifies the provider is used for quality improvement or external reporting.

6. ACCESS TO AND DISCLOSURE OF IMMUNIZATION REGISTRY INFORMATION

This document defines access as having the authorization and capability to enter and/or review system information. Registry access by authorized users is dependent on having a legitimate need for immunization related information on a specific individual. Technical support persons may also access the registry to perform their jobs. Disclosure refers to the release of information to and from the registry. In cases where users have electronic access to the system, the terms "access" and "disclosure" become virtually synonymous in meaning. In other situations, disclosure of information may require the active participation of a registry staff member through such means as telephone responses, preparation of special reports, or preparation of data files. For example, providers whose electronic access to a registry fails will likely then need to telephone the registry for needed information. The responsibility for protecting confidentiality extends to anyone who has access to information contained in the registry, even if they do not access it directly.

Redisclosure is the disclosure by a third party recipient of disclosed information from the registry without the authorization of the person. Privacy protection should follow the information. All recipients of information from the registry except the relevant parents, guardians and children, should be bound by the protections and limitations attached to the information at the initial point of collection.[24]

A. Authorized User Access

Authorized users are those individuals or organizations that require regular access to immunization-related information on a specific individual to provide immunization services. Authorized users may include health care providers, state and local health departments, managed care organizations, school nurses or clinics, and parents. Under appropriate circumstances, non-health care providers such as child care facilities, schools, colleges, WIC programs, and researchers can be authorized users. For example, an authorized school official, such as a school nurse, might use a registry to make necessary immunization determinations on students without specific requests from parents to providers to release the information. Authorized users may also include individuals who provide technical support to the registry.

B. Requests From Individuals And Organizations That Are Not Authorized Users

The Secretary's recommendations state that with very few exceptions, health care information should only be disclosed for health purposes. The recommendations also acknowledge that researchers, service organizations, quality care organizations, and others have legitimate needs for access to personal health care information to advance science, process claims transactions, combat fraud and abuse, and for other purposes. The Secretary has recommended that federal privacy legislation should not interfere with the well established procedures of the criminal justice system; legislation should permit the disclosure of health information without patient authorization for purposes required by state law, such as the reporting of gunshot wound victims, the identification or location of an injured fugitive, or for the investigation of fraud and abuse.

The Secretary has also recommended that with very few exceptions, health care information should only be used for purposes compatible with and directly related to the purposes for which the information was collected or received. Since the purpose of the registry is to ensure that children are appropriately immunized, NVAC has recommended that the use of registry information in a manner that is punitive to parents, such as INS tracking of immigrants, be prohibited.[25]

Law enforcement may be able to obtain registry information under certain circumstances. For example, immunization registry information may be subject to a subpoena or to a court order. However, not all subpoenas are appropriate requests for information. Policies and procedures should ensure that registry staff do everything possible to protect confidentiality while complying with existing laws and regulations. For example, those requesting information contained in the registry may be referred to the provider or to the original source of the information. In addition, all requests from law enforcement agencies and attorneys should be referred to the registry's legal counsel.

C. Minimum Specifications for Access to and Disclosure of Registry Information:

Immunization registry policies and procedures must:

1. clearly define who will have access to registry information, and to which information they will have access.

2. ensure that only authorized users may provide information to the registry or receive information from the registry (see #10 and #11).

3. ensure that every authorized registry user signs a user agreement (see above).

4. ensure that authorized users who provide direct service only access records on children or patients under their care or for whom they share clinical responsibility.

5. ensure that authorized users who finance and/or manage care (e.g., managed care organizations) only access records on children or patients that are enrolled in their plan.

6. ensure that parents and guardians have access to their own children's records unless there is substantial evidence that the information in the record (e.g., child's address) if released, could reasonably be expected to cause harm to the child or others. In such cases, there must be a procedure for determining whether there is substantial evidence of potential harm to the child or others (see implementation guidelines below).

7. ensure that registries provide immunization information directly to parents or guardians requesting such information, unless the parent or guardian requests that the information be sent elsewhere (e.g., school, provider).

8. ensure that parents and guardians have an opportunity to request a correction and/or amendment to the child's record.

9. ensure that in the rare case that parents or guardians are denied the right to inspect, copy, correct or amend the record (see above), the parent or guardian must be receive written notification of the reasons for the denial. Parents and guardians must be able to appeal such denials.

10. ensure that there are procedures for addressing requests for information from individuals and organizations that are not authorized users (e.g., researchers).

11. ensure that law enforcement access to the registry is limited to legally mandated circumstances (see # 12).

12. ensure that all subpoenas, requests for production, warrants, and court orders are immediately referred to legal counsel. Registries must make every reasonable effort, in conjunction with legal counsel, to limit disclosure of information through these means.

13. ensure that individuals are notified in a timely manner when there is a request for personally identifiable information from an individual or organization that is not an authorized user, and in the event of a breach of confidentiality or security if their child's record was involved.

14. ensure that anyone who rediscloses registry information notifies the recipient of the confidential nature of the information (see implementation guidelines below).

15. ensure that registry information that is redisclosed is accompanied by a statement that

notifies the recipient of the following:

that the information disclosed may be from a confidential record protected by state and federal laws,

any further disclosure of the information in an identifiable form may be prohibited without the written, informed consent of the person who is the subject of the information or as permitted by federal or state law, and

unauthorized disclosure of the information may result in significant criminal or civil penalties, including imprisonment and monetary damages.

D. Implementation Guidelines for Access to and Disclosure of Immunization Registry Information

1. Whenever possible, information that is not personally identifiable should be disclosed in response to inquiries.

2. All disclosures should be restricted, to the extent practicable, to the minimum amount of information which the person making the disclosure reasonably believes is necessary to accomplish the intended purpose. Different users may have different levels of access. For example, school nurses may have "read only" access, in order to determine the names of students who are not immunized. In most cases, the location of the child's residence or where the shot was received is not necessary.

3. The policy should delineate how much unique patient information an authorized user is required to enter into the system before access to that patient's immunization record is granted.

4. Evidence of substantial harm includes, but is not limited to evidence that the child or the person responsible for the child has:
   1) been a victim of domestic violence;
   2) contacted a law enforcement official regarding domestic violence as evidenced by a police report involving domestic violence or other physical abuse;
   3) obtained a temporary restraining order to protect the individual from future physical abuse; or
   4) filed other criminal or civil legal proceedings regarding physical protection.

5. Procedures for limiting access to registry information include but are not limited to:

   releasing medically necessary immunization information without demographic information that identifies the family's location, and

   referring the individual (other than parents or guardians) to the provider or the original source of the information.

6. If the content of a record is disputed, the parent or guardian should be allowed to supplement the existing record.

7. Confidentiality policies should address appropriate procedures for faxed and paper transmissions (e.g., calling ahead to verify the fax number, verification receipt of fax, including proper cover sheets for mail and fax).

8. Recipients of redisclosed registry information should be bound by the same confidentiality provisions as the registry (see minimum specification for access and disclosure # 15).

9. Technical and administrative security safeguards consistent with the Secretary of Health and Human Service's standards and HIPAA should be developed to ensure appropriate access to the registry (e.g., passwords, user ID). (See Appendix D).

7. PENALTIES FOR UNAUTHORIZED DISCLOSURES

Accountability is one of the key principles that provide the foundation for the Secretary's recommendations to Congress. The recommendations state that federal legislation should provide severe punishment for those who misuse personal health information, including civil and criminal penalties, and redress for those who are harmed by its misuse. In addition, alternative dispute resolution procedures should be available for civil disputes.

The updated 1997-1998 CDC survey indicates that six state laws that authorize immunization registries or the sharing of immunization information explicitly provide penalties for the improper disclosure of information from the registry or for the improper sharing of immunization information. In addition, numerous state confidentiality laws and computer fraud laws also provide penalties for the improper use and disclosure of confidential information. The survey also indicates that nine state laws specifically provide some type of immunity from civil and/or criminal liability for providers and other health care professionals who disclose information to the immunization registry in good faith.

NVAC recommends that strong penalties for the unauthorized use of registry data should be in place and consistently enforced. Currently, registries use a variety of penalties including the revocation of authorized user privileges, the termination of a contract, professional sanctions, and disciplinary action, up to and including termination of employment.

A. Minimum Specifications for Penalties:

1. Confidentiality policies must clearly define what constitutes a breach of confidentiality.

2. Confidentiality policies must specifically delineate the penalties for the inappropriate use or disclosure of information, and to whom the penalties apply (e.g., individuals, supervisors, organizations).

3. Confidentiality policies must state the applicable penalties contained in existing laws, regulations, and policies.

4. Contracts with independent contractors, vendors, consultants, and others who have access to the registry must delineate penalties for the improper use and disclosure of registry information.

5. Penalties must not be imposed for the good faith disclosure of immunization information to the registry.

6. Penalties must be enforced.

.

8. DATA RETENTION AND DISPOSAL

A. Minimum Specifications for Data Retention and Disposal:

1. Confidentiality policies must address the period of time the information may be held in the registry and whether it will be deleted or archived at the end of that period.

2. Registries must have a written policy that provides for the appropriate storage and disposal of all forms of confidential records (e.g., locked storage cabinets, shredding, recycling, disks).

3. Technical security safeguards consistent with the Secretary of Health and Human Service's standards and HIPAA should be developed to ensure appropriate storage and disposal of records (see Appendix D).

3: FUTURE ISSUES

The policies in this chapter are based on the NVAC recommendations, the experience of registry developers in the public and private sector, as well as that of representatives from CDC National Immunization Program, All Kids Count, the National Vaccine Program Office, state and local health departments and others. The Department of Health and Human Services will publish a final privacy rule in the near future. Although the deadline in HIPAA for Congress to enact privacy legislation has passed, Congress can still enact such legislation. While privacy regulations will be narrower in scope than legislation, it is not clear how legislation or regulations will impact immunization registry development and operation. It will be important to closely monitor developments at the national level.

This chapter does not address several privacy and confidentiality issues that are extremely important for registries. These issues include, but are not limited to:

> The interstate exchange of immunization information: Presently, states with stringent legal protections for confidential health care information may not allow disclosure to states with less protective laws. This issue requires further exploration and study to facilitate the successful operation of immunization registries.
>
> Immunization registries that are part of larger, integrated health information systems: It will be important to assess whether the minimum specifications in this chapter appropriately address registries that are part of integrated information systems. For example, notice might have to be modified.
>
> The relationship of managed care to immunization registries: As managed care participation in registries increases, it will be important to assess and clarify several important issues such as who in the managed care organization should be authorized to access the registry, issues associated with the interstate data collection by managed care organizations, and data submission by managed care organizations in order to avoid dual data entry at the immunization provider level.
>
> Removal of children's records from the registry: At the present time, most immunization registry developers are concentrating on populating registries. Some registries plan to keep information on adults; other registries plan to archive information. The issue of whether 18 year olds should be notified that they are in the registry or that their information will be archived needs to be explored, as well as the impact of state laws addressing the retention of medical records.

As registries continue to develop and the health care system continues to change, new issues will arise. CDC, All Kids Count, and many people in the public and private sector recognize the need for more information and continued dialogue about these issues, in order to continue to ensure the privacy of registry participants and the confidentiality of information contained in registries. Representatives from CDC, All Kids Count, and other organizations are exploring ways to facilitate further discussion about these important issues.

4: TEN KEY ACTION STEPS TO ENSURE PRIVACY AND CONFIDENTIALITY

To protect the privacy of registry participants and the confidentiality of information contained in immunization registries, registry developers and policymakers should take the following action steps:

1. Obtain a review by expert legal counsel on the applicability of all relevant federal, state, local, or other (e.g., military) laws, regulations and policies. Particular attention should be given to those pertaining to the privacy and confidentiality of medical records.

2. Identify potential areas of confusion or omission in existing laws, regulations, and policies, in order to comply with the required minimum specifications.

3. Determine whether existing laws or rules need to be clarified to specifically address immunization registries.

4. Prepare or revise a written confidentiality policy. This document should be based upon the best interpretation by legal counsel of existing and proposed laws, regulations, and policies.

5. Seek community input and input from privacy experts to best ensure that the policy represents a fair balance between protecting the community through high immunization rates and protecting individuals' privacy.

6. Ensure that all critical terms are adequately defined within the confidentiality policy to prevent misinterpretation.

7. Determine an acceptable approach for implementing the minimum specifications in a manner that is consistent with community norms and values.

8. Have a technical person or persons review the confidentiality policy to provide input and ensure that the policy is technically feasible.

9. Incorporate a specific requirement that the confidentiality and security policies are formally reviewed and reevaluated at set time intervals. Ensure that there is a procedure in place to update them and reeducate the public and users concerning relevant changes.

10. Ensure that appropriate penalties for unauthorized use and disclosure of confidential information are in place and consistently enforced.

GLOSSARY

Access is the authorization and capability to enter and/or review system data.

Authorized users are those individuals or organizations that require regular access to immunization-related information on a specific individual to provide immunization services. Authorized users may include health care providers, state and local health departments, managed care organizations, schools, and parents. Under appropriate circumstances, non-health care providers such as child care facilities, schools, colleges, WIC programs, researchers, and individuals who provide technical support to the registry can be authorized users.

Confidentiality is the treatment of information that an individual has disclosed in a relationship of trust with the expectation that it will not be divulged to others in ways that are inconsistent with the understanding of the original disclosure.

Confidentiality statement is a written statement, dated and signed by an individual which certifies that the individual has received a copy of the confidentiality policy, understands the terms, and agrees to comply with the policy.

Disclosure refers to the release of information to and from the registry.

Explicit consent or "opt in": Registries using this option will only include immunization information in the registry if the parent or guardian explicitly consents to participation in the registry. Written and verbal consent are used.

Implied consent or "opt out": Registries using this option automatically include all children in the registry unless a parent or guardian requests otherwise. A parent or guardian who does not wish to participate may choose to "opt out." Verbal or written methods of opting out may be required.

Individually identifiable information is information that identifies the individual, or can reasonably be used to identify the individual.

"Locked or restricted access": Registries using this option keep the demographic and immunization information in the registry but upon the request of the parent or guardian, it is not shared.

Non-identifiable health information is health information from which personal identifiers have been removed, masked, encrypted or otherwise concealed, such that the information can not reasonably be expected to identify individual patients.

Notification informs patients and their parents or legal guardians of the purpose and potential uses of the immunization registry.

Parent is a person who can legally give consent for the child's immunization.

Personally identifiable information is information that identifies the individual, or can reasonably be used to identify the individual.

Privacy is the legal right of an individual to limit access by others to some aspect of the person.

"Read only" access is a type of access to the registry which allows the user to view specified information contained in the registry. Users with read only access are not able to add, delete, or alter any information in the registry.

Redisclosure is the disclosure by a third party recipient of disclosed health information without the authorization of the person.

Reminder/ recall notices are notification to parents or guardians about immunizations currently needed or past due for their child.

Security encompasses a set of technical and administrative procedures designed to protect data systems against unwarranted disclosure, modification, or destruction.

User agreement defines the terms under which individuals and organizations become authorized immunization registry users; it includes the obligations and responsibilities of both parties.

ABBREVIATIONS USED IN THIS CHAPTER

AKC- All Kids Count

CDC- Centers for Disease Control and Prevention

COSSMHO- National Coalition of Hispanic Health and Human Services Organizations

INS- Immigration and Naturalization Service

HIPAA- Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191)

NIP- National Immunization Program

NVAC- National Vaccine Advisory Committee

NVPO- National Vaccine Program Office

RWJF- Robert Wood Johnson Foundation

WIC- Women, Infants and Children Nutrition Supplement Program

APPENDIX A: THE NVAC RECOMMENDATIONS

The NVAC approved report, Development of Community- and State-Based Immunization Registries includes the following recommendations which were developed to ensure the appropriate protection of privacy and confidentiality for individuals and the security of information contained in immunization registries:

1. Protection of privacy and maintenance of confidentiality are essential to the successful development of immunization registries. Registry developers must give careful consideration to privacy and confidentiality issues to reflect the values and special needs of the communities they serve.

2. Registry developers must give special consideration to the privacy and confidentiality needs of immigrant communities.

3. Federal legislation to establish a minimum set of privacy/confidentiality standards would be very helpful. To assist in the development of registries that can exchange data while also ensuring privacy and confidentiality, the federal government should work with key stakeholders to develop and disseminate model privacy and confidentiality policies and legislation for registries.

4. At a minimum, immunization registries should:

Ensure that patients/parents are notified of the existence of a registry and of the information contained in the registry
Inform patients/parents of the purpose and potential uses of the registry
Permit patients/parents to review and amend information in the registry
Accept responsibility for reliability and protection of registry information

5. Parents must be given the option to decide whether or not their children will participate in a registry. In some communities, parents are informed of the registry and its purposes and potential uses during routine educational sessions offered at the birth hospital. At this time, or at any later time, parents should be allowed to opt out of a registry. In communities where the "opt in"/informed consent approach is most consistent with community values, this is the option that should be offered. Parents should not be penalized for choosing not to participate in a registry for religious, philosophical, privacy, or other reasons.

6. Registry developers should limit access to registry information and maintain audit trails to monitor access to records. Individuals should have access to their own records and to these audit trails.

7. Strong penalties for the unauthorized use of registry data should be in place and uniformly enforced.

8. Use of registry data in a manner that is punitive to parents/patients (e.g., denial of health insurance/coverage, INS tracking of immigrants, other law enforcement purposes) must be prohibited.

9. If registries are to be integrated with larger health information systems, protection

of privacy and confidentiality must be ensured.

10. The federal government should support an ongoing independent assessment of the benefits, risks, and costs of registry development and implementation with regard to issues including privacy and confidentiality.

APPENDIX B: MINIMUM SPECIFICATIONS FOR THE PROTECTION OF PRIVACY AND CONFIDENTIALITY

1. Confidentiality Policies:

1. Every immunization registry must have a written confidentiality policy that will be made available upon request.
2. The confidentiality policy must be reviewed to ensure that it is consistent with applicable Federal, State, and local laws and regulations.
3. Confidentiality policies must apply to everyone who has authorized access to the registry.
4. Confidentiality policies must apply to all individually identifiable information in all formats including paper-based and electronic records.
5. Confidentiality policies must prohibit the unauthorized redisclosure of personally identifiable information.
6. Confidentiality policies must:
   - clearly define the user's responsibility to maintain confidentiality
   - clearly define what constitutes a breach of confidentiality**,** and
   - specifically delineate the penalties for the inappropriate use or disclosure of information.
7. Confidentiality policies must be actively enforced.

2. User Agreements and Confidentiality Statements:

1. All authorized immunization registry users must receive a copy of the confidentiality policy.
2. All individuals with access to the immunization registry must either:
   - sign a confidentiality statement or a user agreement indicating that they understand the terms of the confidentiality policy, including the penalties for violation of the policy, and they agree to comply with the policy, or
   - individuals must operate under an employer who has signed an agreement indicating that they are responsible for the actions of the staff.
3. Confidentiality statements and user agreements must specify the time period covered by the statement or agreement**,** and they must be renewed on a regular basis.
4. Confidentiality statements and user agreements must specify the user's level of access to information in the immunization registry.

3. Notification:

1. Information about the existence of the immunization registry (notification/notice) must be provided directly to patients and/or their parents or legal guardians.
2. Notification must include the following:
   - what information will be contained in the registry
   - what the information will be used for
   - with whom the information will be shared
   - the definition of participation in the registry and how to exercise choice about participation
   - procedures for review and correction or amendment of information
   - contact information for further questions
3. Notification must be in language the parent or guardian can understand.

4. Information about the immunization registry must be given to the patient and/or parent or guardian before any immunization information is included in the registry.
5. In states where immunization registries are populated directly from vital records:
   a) if only demographic information is transmitted, parents or guardians must be notified before any immunization information is included in the registry, and
   b) if information on vaccines given at birth, such as HepB, is transmitted in addition to the demographic information, parents or guardians must be notified before this information is included in the registry.
6. If a parent or guardian signs a contract with a health care provider or health plan and that entity participates in the registry, the policy contract or health plan brochure does not provide sufficient notice. Providers must provide additional notice consistent with the minimum specifications.

4. Choice:

1. Parents must be able to choose whether or not to participate in the registry, and they must be able to change this decision at any time.
2. Parents and children must not be penalized for choosing not to participate in a registry for religious, philosophical, privacy or other reasons.
3. Personally identifiable information of those who have chosen not to participate must not be shared.
4. The options and benefits regarding participation must be clearly explained to parents or guardians.
5. Verbal choice about participation in the registry must be documented.
6. The decision whether or not to vaccinate, and the decision whether or not to participate in the registry are separate and distinct decisions. Therefore, separate signatures must be used to indicate consent or refusal to vaccinate and for consent or opting out of participation in the registry.

5. Use of Immunization Registry Information:

1. Each registry must identify the purposes for which it is collecting immunization information, and inform all authorized users and parents or guardians.
2. Information in the immunization registry must only be used for the purposes for which it was collected.
3. Immunization registry developers and managers must make every reasonable effort to ensure that immunization information is not used in a punitive manner (e.g., to deny services or to track immigration status). (See minimum specifications for disclosure).
4. Providers must be notified and given the opportunity to consent if immunization registry information that identifies the provider is used for quality improvement or external reporting.

6. Access to and Disclosure of Registry Information:

Immunization registry policies and procedures must:

1. clearly define who will have access to registry information, and to which information they will have access.
2. ensure that only authorized users may provide information to the registry or receive information from the registry (see #10 and #11).
3. ensure that every authorized registry user signs a user agreement (see above).
4. ensure that authorized users who provide direct service only access records on children

or patients under their care or for whom they share clinical responsibility.

5. ensure that authorized users who finance and manage care (i.e., managed care organizations) only access records on children or patients that are enrolled in their plan.
6. ensure that parents and guardians have access to their own children's records unless there is substantial evidence that the information in the record (e.g., child's address) could reasonably be expected to cause harm to the child or others. In such cases, there must be a procedure for determining whether there is substantial evidence of potential harm to the child or others (see implementation guidelines below).
7. ensure that registries provide immunization information directly to parents or guardians requesting such information, unless the parent or guardian requests that the information be sent elsewhere (e.g., school, provider).
8. ensure that parents and guardians have an opportunity to request a correction and/or amendment to the child's record.
9. ensure that in the rare case that parents or guardians are denied the right to inspect, copy, correct or amend the record (see above), the parent or guardian must be receive written notification of the reasons for the denial. Parents and guardians must be able to appeal such denials.
10. ensure that there are procedures for addressing requests for information from individuals and organizations that are not authorized users (e.g., researchers).
11. ensure that law enforcement access to the registry is limited to legally mandated circumstances (see # 12).
12. ensure that all subpoenas, requests for production, warrants, and court orders are immediately referred to legal counsel. Registries must make every reasonable effort, in conjunction with legal counsel, to prevent disclosure of information through these means.
13. ensure that individuals are notified in a timely manner when there is a request for personally identifiable information from an individual or organization that is not an authorized user, and in the event of a breach of confidentiality or security if their child's record was involved.
14. ensure that anyone who rediscloses registry information notifies the recipient of the confidential nature of the information (see implementation guidelines below).
15. ensure that registry information that is redisclosed is accompanied by a statement that notifies the recipient of the following:

    that the information disclosed may be from a confidential record protected by state and federal laws,

    any further disclosure of the information in an identifiable form may be prohibited without the written, informed consent of the person who is the subject of the information or as permitted by federal or state law, and

    unauthorized disclosure of the information may result in significant criminal or civil penalties, including imprisonment and monetary damages.

7. Penalties:

1. Confidentiality policies must clearly define what constitutes a breach of confidentiality.
2. Confidentiality policies must specifically delineate the penalties for the inappropriate use or disclosure of information, and who the penalties apply to (e.g., individuals, supervisors, organizations).
3. Confidentiality policies must state the applicable penalties contained in existing laws, regulations, and policies.

4. Contracts with independent contractors, vendors, consultants, and others who have access to the registry must delineate penalties for the improper use and disclosure of registry information.
5. Penalties must not be imposed for the good faith disclosure of immunization information to the registry.
6. Penalties must be enforced.

8. Data Retention and Disposal:

1. Confidentiality policies must address the period of time the information may be held in the registry and whether it will be deleted or archived at the end of that period.
2. Registries must have a written policy which provides for the appropriate storage and disposal of all forms of confidential records (e.g., locked storage cabinets, shredding, recycling, disks).
3. Technical security safeguards consistent with the Secretary of Health and Human Services' standards and HIPAA should be developed to ensure appropriate storage and disposal of records.

APPENDIX C: CALIFORNIA DISCLOSURE LANGUAGE

[PROTOTYPE LANGUAGE FOR HEALTH CARE PROVIDER'S DISCLOSURE TO PATIENT OR PARENT/GUARDIAN ON IMMUNIZATION RECORD SHARING WITH REGISTRIES

As required by Health and Safety Code Section 120440
***Immunization Branch, California Department of Health Services, July 19, 1999*]**

This office/clinic will share some information on your child with the local health department immunization registry and the state health department, unless you refuse to allow this. The registry may share this information with other doctors, clinics or hospitals your child goes to for care, <u>if</u> they ask for it. The only information we will share is:

> **Your and your child's name, your child's birthplace, vaccines he or she has received, any serious reaction he or she had to a vaccine, your address and phone number, and other non-medical information if needed to make sure it is the correct person's record.**

The doctors, clinics or hospitals which get this information can use it only to:

- **help in deciding what vaccines your child needs;**
- **phone or send you a reminder when a vaccine is due; and**
- **tally numbers of patients who are or are not up-to-date on their vaccines (without patient names, addresses, etc., included).**

The registry may also share the same information, <u>without your address or phone number</u>, with schools, child care centers, WIC supplemental food clinics, or health care plans, <u>if</u> they ask for it. These places can use that information only for the reasons listed above, and (a) for schools or child care centers, to help you prove your child has had the vaccines required for entry, (b) for WIC clinics, to let you know if your child has vaccine doses due, and (c) for health care plans, to help process insurance payments.

All of these people and groups listed above who ask for and get this information are required by law to keep it confidential and use it only for the reasons listed above. Also, you have these rights:

- **To refuse to have us share any of this information now or at any time.**
- **To refuse to get reminder notices when vaccines are due.**
- **To look at your child's record at the health department registry and correct any errors.**
- **To get the names and addresses of anyone with whom this information is shared.**

If you wish to refuse to have us share this information, or to refuse to get reminders when your child is due for vaccines, please tell us now.

Thank you.

APPENDIX D: SECURITY OF HEALTH DATA

Protection of the confidentiality of individually identifiable healthcare data depends on a carefully considered plan of security measures to safeguard the data and the plan's vigorous enforcement. Security refers to the measures taken to protect the data from unauthorized access or unwanted change or loss and can include such procedures as audit trails, physical access controls such as passwords, content access controls such as access limitations according to the user's role, and disaster recovery practices. It can also include organizational practices such as training programs and security policies.

As discussed in the body of the Confidentiality chapter update, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires privacy and confidentiality protections for personally identifiable individual health data, either through legislation by Congress or regulation by the Secretary of the Department of Health and Human Services (the Secretary). The Secretary was required to submit recommendations to Congress as it considered privacy legislation. In addition to recommendations on privacy issues, the Secretary's report, which was delivered to Congress on September 11, 1997, discussed the basic obligation of health record holders to safeguard the information through the implementation of security measures.

Those receiving health information should be required to maintain reasonable and appropriate administrative, technical, and physical safeguards to (1) ensure the integrity and confidentiality of health information, and (2) protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized uses or disclosures of the information. The recommendations describe the varied and dynamic technologies in use, which call for different types and degrees of security. The Secretary's recommendation stated that the legislation should not create an obligation of absolute security, but rather measures that were described as reasonable, appropriate, and reasonably anticipated. Those receiving health information should consider the degree of risk, the likely consequences of compromise, and the expenditure, financial and other, required to address the risk. "The measures should especially include employee education, clear and certain punishment for misuse, and technical controls on access to information within an organization, since there is evidence that a substantial threat to information is careless or deliberate misuse by those who have authorized access to it in their normal work activities."

The HIPAA legislation requires the establishment of security standards for health care information systems and standards for electronic signatures. The Notice of Proposed Rule Making (NPRM) for implementing this provision was published on August 12, 1998, for public comment. The requirements of this regulation will apply to any health care provider that electronically maintains or transmits any health information relating to an individual (NPRM Section II.A.), and therefore sets a standard that immunization registries must follow. When the comments have been analyzed, a final rule will be published. The final rule may differ substantially from the NPRM, since the analysis of public comments may lead to a change in direction. The NPRM noted that there was no recognized single standard that addresses all the components of security and identified the following high-level concepts to base the standard on: (1) It must be comprehensive, (2) It must address all aspects of security in a concerted fashion so that if two systems meet the standards and exchange information with each other the overall system is essentially secure, (3) It must be technology-neutral, and (4) It must be scalable. The NPRM references the National Research Council's 1997 report, *For The Record: Protecting*

Electronic Health Information (the Report). The Report recognizes that appropriate security practices depend on individual circumstances and recommends the following:

> "It is therefore not possible to prescribe in detail specific practices for all organizations; rather, each organization must analyze its systems, vulnerabilities, risks, and resources to determine optimal security measures. Nevertheless, the committee believes that a set of practices can be articulated in a sufficiently general way that they can be adopted by all health care organizations in one form or another." (Page 168)

The Report provides recommended organizational and technical policies, practices, and procedures that all organizations that handle patient-identifiable health data should adopt. The organization practices are: (1) Security and confidentiality policies, (2) Information security officers, (3) Education and training programs, and (4) Sanctions. The technical practices are : (1) Individual authentication of users, (2) Access controls, (3) Audit trails, (4) Physical security and disaster recovery, (5) Protection of remote access points, (6) Protection of external electronic communications, (7) Software discipline, and (8) System assessment. In addition, the Report recommended that "the federal government should work with industry to promote and encourage an informed public debate to determine an appropriate balance between the primary concerns of patients and the information needs of various users of health care information."

The HIPAA security NPRM was developed in the spirit of the last recommendation above. It gives a general set of practices that can be implemented, while maintaining a balance between the need to secure health data and the economic cost of securing it. The NPRM presents the requirements in four categories: (1) Administrative procedures, (2) Physical safeguards, (3) Technical security, and (4) Technical security mechanisms. The NPRM presents matrices for each of these, listing the general requirement in one column and possible methods of implementation in another. Each item in the list of requirements is then discussed in greater detail.

Minimum Specifications for Security

Immunization registries should take security measures that are consistent with the Secretary's recommendations on data security. These include actions 1) to maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of health information and 2) to protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized uses or disclosures of the information. To implement this recommendation, at a minimum, each immunization registry should conduct a self-assessment of the potential risks and vulnerabilities of the individual health data in its possession and develop, implement, and maintain appropriate security measures. The assessment and documentation of measures taken should be kept current and should be available to address any security situation or inquiry in connection with the registry.

Guiding Principles for Security

The self-assessment should address at a minimum the four organizational practices and the eight technical practices listed above from the National Research Council's 1997 report.

Resources

There are many sources of information on security measures. Several are listed below.

The NPRM itself provides an excellent discussion of these in a general sense. It does not name particular technologies to accomplish these. The NPRM is available at http://aspe.os.dhhs.gov/admnsimp/seclist.htm.

For The Record: Protecting Electronic Health Information, National Research Council, National Academy Press, 1997. (http://www.nap.edu/readingroom/)

The Computer-Based Patient Record: An Essential Technology for Health Care, Institute of Medicine, National Academy Press, 1997. (http://www.nap.edu/readingroom/)

Health Data in the Information Age, Institute of Medicine, Committee on Regional Health Data Networks, National Academy Press, 1994. (http://www.nap.edu/readingroom/)

A compilation of security standards developed by an accredited standards development organization, the American Society for Testing and Materials (ASTM), is available for purchase (http://www.astm.org). It contains the following standards:

PS100-97 Provisional Standard Specification for Authentication of Healthcare Information Using Digital Signatures

PS101-97 Provisional Standard Guide on Security Framework for Healthcare Information

PS102-97 Provisional Standard Guide for Internet and Intranet Healthcare Security

E 1762-95 Standard Guide for Electronic Authentication of Healthcare Information

E 1869-97 Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information

E1985-98 Guide for User Authentication and Authorization

E 1986-98 Guide for Information Access Privileges to Health Information

E1988-98 Guide for Training of Persons Who Have Access to Health Information

Other ASTM documents include:

PS115-99 Provisional Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems

E1987-98 Guide for Individual Rights Regarding Health Information

Many websites can educate readers about security issues. For example, cryptography questions can be researched at http://www.rsa.com/rsalabs/faq.

Another educational site is http://www.nai.com/asp_set/products/tns/intro.asp.

Another educational site is http://www.microsoft.com/security.

A set of informational documents and position papers published by the Computer-based Patient Record Institute and available on their web site at www.cpri.org/resource/cpri_docs.html.

Guidelines for Establishing Information Security Policies

Guidelines for Information Security Education Programs

Guidelines for Managing Information Security Programs

Sample Confidentiality Statements and Agreements

Glossary of Terms Related to Information Security

Security Features for Computer-based Patient record Systems

Guidelines for Electronic Signature Policies

Action Plan for Addressing Confidentiality and Security Issues in Implementing

Computer-based Patient Record Systems
Access to Patient Data
Authentication in a Computer-based Patient Record

The Health Care Financing Administration's Internet Security Policy, November 24, 1998. Available at http://www.hcfa.gov/security/isecplcy.htm

Discussion and definition of some of the technical security terms and recommendations are provided below.

Individual authentication of users. Access paths to immunization registries should at the very minimum require valid User ID and password for basic authentication. One-time passwords are available for circumstances which call for frequent verification of authenticity. User ID and password schemes, however, are easily compromised when used for authentication on open networks. For this reason, systems using the Internet or large corporate networks should consider the use of digital signatures and two factor authentication as described:

> A **digital signature** (a.k.a. digital certificate), when issued by a verifiable party, is presented by the user when attempting to gain access. If the electronic credentials are identified and trusted, the system will grant the appropriate access rights. This type of verification also provides what is known as a key pair which is used for the session encryption. Using this type of authentication, a system can be certain of the user and source of the access request.
>
> **Two-factor authentication** uses the concept that a user must know something and must have something in order to gain access. Implementations of two-factor authentication use smart cards or other electronic tokens to facilitate the "something you have." A pass-phrase or PIN is typically used as the "something you know." Using these two factors, an immunization registry can be reasonably certain that the person attempting access is the person to whom access should be granted

Access Control. Immunization registries should use the highest level of technology reasonable to the circumstances to gain initial access to the registry; e.g., user id's and passwords, encryption (some publicly available), and enhanced authentication services, such as digital signatures, tokens or smartcards. A system must have suitable management capability to control the access of the system to users, both individual and groups, based on the roles they require when accessing the registry.

Audit Trails. In order to maintain data and access integrity, an audit trail that is safe from tampering (including system administrator) should be maintained by the immunization registry to ensure all events are properly recorded. Audit trails should record each access event and the level at which the event took place (end user, administrator, backup operator, etc) They should provide information as to who accessed the registry, the time of entry, and duration.

Authorization Control. The software management functions of the registry should provide the capability to grant access to users and groups based on their need or role.

Data Authentication. Immunization data transmitted to other registries should contain source

identification data within the transaction or use Public Key technology to authenticate the integrity of the source. This identification data will be generated and deciphered using publicly known algorithms.

Entity Authentication. Immunization registry host sites should apply for electronic credentials offered by a third party, known as a Certificate Authority (CA). The CA would provide all background investigation on the applicant and assure the identity of the applicant presenting the digital signature.

Physical security & disaster recovery. Each provider of registry services should have a written physical security and disaster recovery plan. These plans should be tested and evaluated by third parties to make sure any policies are enforceable and recovery actions are viable.

Protection of external electronic communications. Encryption of data passing over telecommunication paths should be incorporated in immunization registries. The technology allows for use of 128 bit encryption within the United States with little performance overhead. These encryption techniques are scalable and offered at little or no cost to system developers.

Software discipline. Immunization registry software developers should adhere to national standards and conform to normal software development practices. Care should be taken to protect registry software source code from tampering. All code should go through a Quality Assurance process to reduce the entry of code-related problems in the operation of the registry. Electronic releases of the object code should contain digital signatures to ensure its authenticity.

System assessment. Computer-based systems are extremely complex, making configuration-related vulnerabilities the most likely risk of exposure. Using third party solutions, an immunization registry should be tested periodically for configuration-related vulnerabilities.

References

Best Principles for Health Privacy, A Report of the Health Privacy Working Group, Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University, July 1999.

Centers for Disease Control and Prevention National Immunization Program 1999 Annual Immunization Registry Report, April 1999.

Centers for Disease Control and Prevention, Health Communication Evaluation Services, Findings of Focus Group Research on Immunization Registries, December 1998. Available at: http://www.cdc.gov/nip/registry/i_announce.html.

Centers for Disease Control and Prevention, National Immunization Program Survey of State Immunization Registry Legislation. Available at: http://www.cdc.gov/nip/registry/legsurvey.htm.

Confidentiality of Individually Identifiable Health Information, Recommendations of the Secretary of Health and Human services, pursuant to Sec. 264 of the Health Insurance Portability and Accountability Act of 1996, September 11, 1997. Available at: http://aspe.os.dhhs.gov/pvcrec.htm.

Dept. Health and Human Services. Healthy People 2010 Objectives: Draft for Public Comment. Washington DC, 1998.

Development of Community- and State-Based Immunization Registries, Report of the National Vaccine Advisory Committee (NVAC), January 12, 1999. Available at: http://www.cdc.gov/nip/registry/i_recs.htm.

Health Insurance Portability and Accountability Act of 1996. Pub. L. No. 104-191 (August 21, 1996).

Institute of Medicine (US). Health data in the information age. Washington DC: National Academy Press, 1994.

Model State Public Health Privacy Act, with comments [as of February 19, 1999], Model State Public Health Privacy Project, Georgetown University Law Center. Available on the World Wide Web at: http://www.critpath.org/msphpa/modellaw3.htm.

Privacy Act of 1974. Pub L. No. 93-579 (December 31, 1974).

Privacy, Confidentiality, and Security in Information Systems of State Health Agencies, O'Brien DG, Yasnoff WA. Am J Prev Med 1999;16(4).

Protecting privacy in computerized medical information. Washington DC: US Congress, Office of Technology Assessment; 1993. Publication OTA-TCT-576.

Remarks by the President in announcement on immunization-child care, July 23, 1997. Available at: http://www.cdc.gov/nip/announce/clinton.htm

Endnotes

1. Dept. Health and Human Services. Healthy People 2010 Objectives: Draft for Public Comment. Washington DC, 1998.

2. Dept. Health and Human Services. Healthy People 2010 Objectives: Draft for Public Comment. Washington DC, 1998.

3. Centers for Disease Control and Prevention National Immunization Program 1999 Annual Immunization Registry Report, April 1999.

4. Development of Community- and State-Based Immunization Registries, Report of the National Vaccine Advisory Committee (NVAC), January 12, 1999. Available at: http://www.cdc.gov/nip/registry/i_recs.htm.

5. Institute of Medicine (US). Health data in the information age. Washington DC: National Academy Press, 1994.

6. Development of Community- and State-Based Immunization Registries, Report of the National Vaccine Advisory Committee (NVAC), January 12, 1999. Available at: http://www.cdc.gov/nip/registry/i_recs.htm.

7. Development of Community- and State-Based Immunization Registries, Report of the National Vaccine Advisory Committee (NVAC), January 12, 1999. Available at: http://www.cdc.gov/nip/registry/i_recs.htm.

8. Health Insurance Portability and Accountability Act of 1996. Pub. L. No. 104-191 (August 21, 1996).

9. Confidentiality of Individually Identifiable Health Information, Recommendations of the Secretary of Health and Human services, pursuant to Sec. 264 of the Health Insurance Portability and Accountability Act of 1996, September 11, 1997. Available at: http://aspe.os.dhhs.gov/pvcrec.htm.

10. Remarks by the President in announcement on immunization-child care, July 23, 1997. Available at: www.cdc.gov/nip/announce/clinton.htm.

11. Centers for Disease Control and Prevention, Health Communication Evaluation Services, Findings of Focus Group Research on Immunization Registries, December 1998. Available at: http://www.cdc.gov/nip/registry/i_announce.html.

12. Centers for Disease Control and Prevention, Health Communication Evaluation Services, Findings of Focus Group Research on Immunization Registries, December 1998. Available at: http://www.cdc.gov/nip/registry/i_announce.html.

13. Protecting privacy in computerized medical information. Washington DC: US Congress, Office of Technology Assessment; 1993. Publication OTA-TCT-576.

14. Development of Community- and State-Based Immunization Registries, Report of the National Vaccine Advisory Committee (NVAC), January 12, 1999. Available at: http://www.cdc.gov/nip/registry/i_recs.htm.

15. Records, Computer and the Rights of Citizens. Department of Health, Education and Welfare (US), Secretary's Advisory Committee on Automated Personal Data Systems; 1973.

16. Development of Community- and State-Based Immunization Registries, Report of the National Vaccine Advisory Committee (NVAC), January 12, 1999. Available at: http://www.cdc.gov/nip/registry/i_recs.htm.

17. Centers for Disease Control and Prevention, National Immunization Program Survey of State Immunization Registry Legislation. Available at: http://www.cdc.gov/nip/registry/legsurvey.htm.

18. Development of Community- and State-Based Immunization Registries, Report of the National Vaccine Advisory Committee (NVAC), January 12, 1999. Available at: http://www.cdc.gov/nip/registry/i_recs.htm.

19. Development of Community- and State-Based Immunization Registries, Report of the National Vaccine Advisory Committee (NVAC), January 12, 1999. Available at: http://www.cdc.gov/nip/registry/i_recs.htm.

20. Development of Community- and State-Based Immunization Registries, Report of the National Vaccine Advisory Committee (NVAC), January 12, 1999. Available at: http://www.cdc.gov/nip/registry/i_recs.htm.

21. Development of Community- and State-Based Immunization Registries, Report of the National Vaccine Advisory Committee (NVAC), January 12, 1999. Available at: http://www.cdc.gov/nip/registry/i_recs.htm.

22. Development of Community- and State-Based Immunization Registries, Report of the National Vaccine Advisory Committee (NVAC), January 12, 1999. Available at: http://www.cdc.gov/nip/registry/i_recs.htm.

23. Development of Community- and State-Based Immunization Registries, Report of the National Vaccine Advisory Committee (NVAC), January 12, 1999. Available at: http://www.cdc.gov/nip/registry/i_recs.htm.

24. Best Principles for Health Privacy, A Report of the Health Privacy Working Group, Health Privacy Project, July 1999.

25. Development of Community- and State-Based Immunization Registries, Report of the National Vaccine Advisory Committee (NVAC), January 12, 1999. Available at: http://www.cdc.gov/nip/registry/i_recs.htm.